Leaky Sensor Fields: Deviating, Accelerating, and Restraining the Smart Home

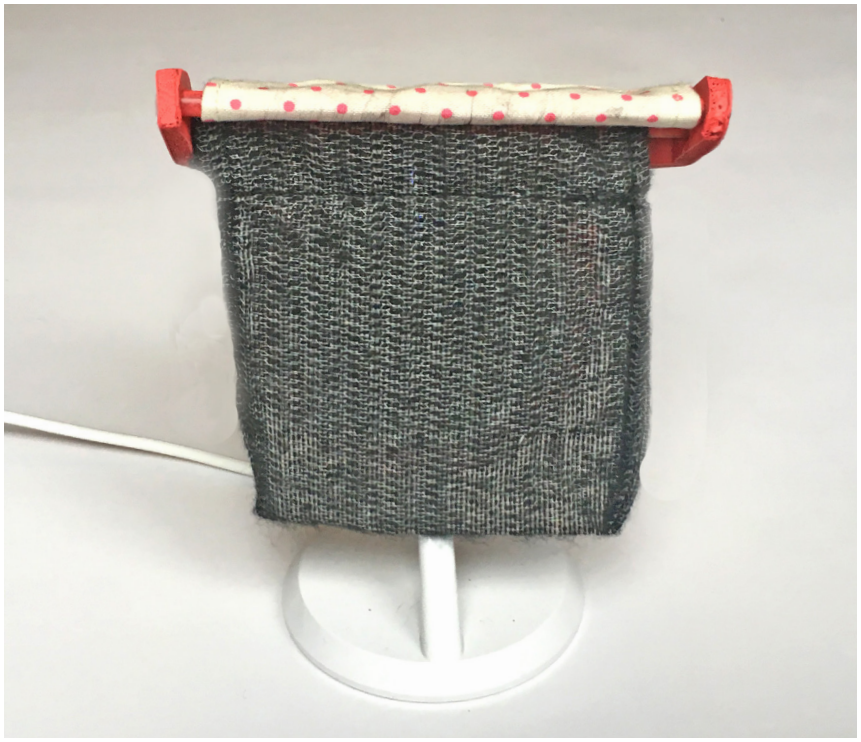
James Pierce

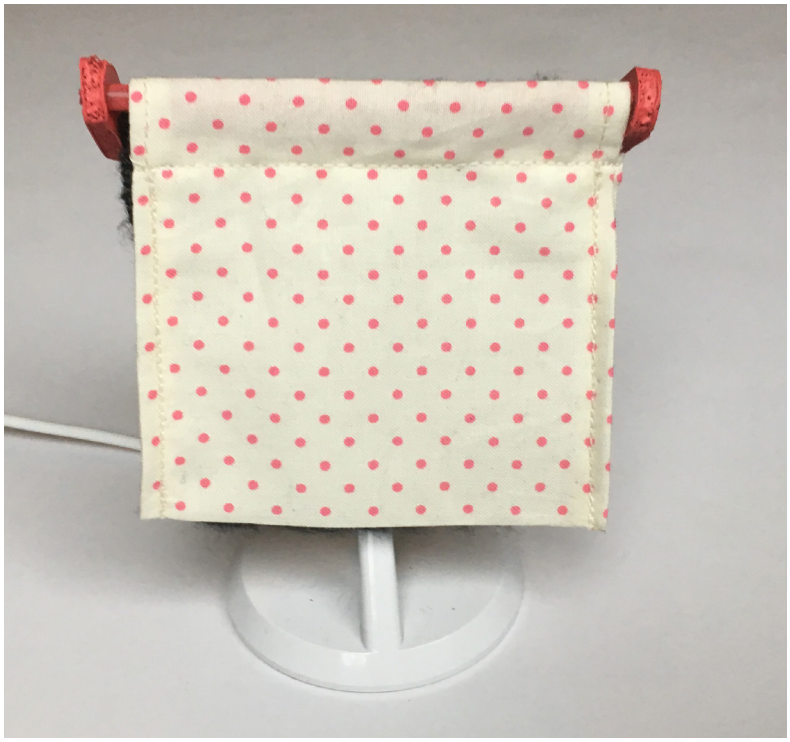
California College of the Arts, San Francisco, USA
jpierce@cca.edu

University of California, Berkeley, USA
pierjam@berkeley.edu

Abstract: This project examines the proliferation of leaky sensor fields by studying and redesigning smart home security cameras. This work begins with a set of close Based on close studies of existing smart home security cameras, Through a series of design explorations that accelerate, diverge, and restrain smart cameras, this research then explores scenarios to help us speculate about the future of smart homes and as ways of understanding the present.

Keywords: Internet of Things (IoT), privacy, security, speculative design, critical design, design research, smart home, smart city






amazon

Introduction

In 2001, when asked about the possibility of a Google "implant" technology, then CEO Eric Schmidt responded by stating that "Google policy ... is to get right up to the creepy line—but not cross it" (Cole, 2012). In formulating this response, Schmidt sketches the contours of an important concept for engaging with social and ethical issues bound up with technology—including many topics that have become important subjects of design research, such as privacy and security (Shklovski et al, 2016), technology anxieties (Pierce and DiSalvo, 2018), civic IoT (Jenkins, 2017; Davoli and Redstrom, 2015) and design methods for engaging smart things (Giaccardi et al, 2016, Wakkary et al, 2018).

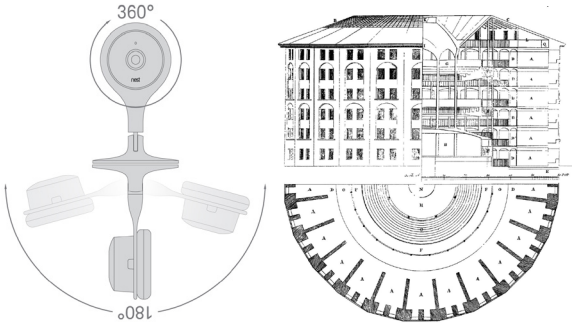


Figure. *Nestopticon.* Image composite of two diagrams from 2018 Nest informational materials adjacent to Jeremy Bentham's Panopticon penitentiary, architectural proposal by Willey Reveley, 1979. [Image credit: James Pierce]

Creepiness is not merely a useful and commonly used concept for pressure testing and publicly debating the social and ethical implications of new technologies. Creepiness also functions as a device for *registering* social and ethical concerns. Wherever creepiness is felt, murmured, or shouted out loud, we are sure to find complex social and ethical problems, issues, and dilemmas. Creepiness is intriguing in part because it is felt before it is reflectively articulated or intellectually argued. The affective feeling of creepiness experienced at the personal, bodily level is often relayed and broadcast through news headlines, social media, and cultural touchstones such as science fiction films and literature. Within Human-Computer Interaction (HCI) and Design Research, Shklovski et al. have drawn attention to the significance and prevalence of users' experiences of creepiness when tracked by their smartphones (Shklovski et al, 2016). Based on interview data, Shklovski et al observe that "despite potentially positive outcomes of this kind of tracking, the public response remains negative often because people simply find it creepy. At the same time, people continue to use the technologies ... even as they express outrage" (2347). Building on this work, Pierce and DiSalvo isolate creepiness as a pivotal "network anxiety" and use it as a "central node through which to connect and route other more troubling effects" (Pierce and DiSalvo, 2018, 4). This research follows these tingling sensations and intellectual reflections on creepiness, taking Schmidt's creepy line as a preliminary point of departure.

The key question guiding this inquiry is twofold. First, in what ways is the smart home creepy: Where and how are the current lines of creepiness drawn? Second, how does design work to manage creepiness and achieve social acceptance of technology—often by mitigating or suppressing fears, anxieties, and harms? In partial answer to the big questions, this design research project develops the concept of *digital leakage* as the propensity for digital information to be shared, stolen, and misused in ways unbeknownst or even harmful to those to whom the data pertains or belongs. This paper begins by looking closely at the lens and sensor data of smart cameras, tracing the effects of *leaky sensor fields*. The project then delves in controversial applications and possible future trajectories of smart cameras.

This paper concludes by revealing an underlying framework guiding this inquiry. The major cases studies presented here proceed along three key *redirective design: divergently* and deviationally into the absurd and exaggerated, *accelerating* past plausible or expected near-term projections, and productively *restraining* and reversing the ratcheting up effects of technological advancement.

This work extends and amplifies the author's prior work focused on verbally articulating the concepts outlined above (Pierce, 2019, Pierce and DiSalvo, 2018). This paper offers many new and expanded design proposals and prototypes and focuses on the details, process, and uses of the designs.

In addition to "physical 3D" prototyping, this research follows a long tradition of design proposals, sketches, diagrams, and montages. The prototypes presented in the final pages of this paper are not the final results of the process, but rather focal points amid a constellation of visual/textual studies and explorations (a *selection* of which are presented here). The totality of this work will be exhibited at RtD—including print and screen-based artifacts.

Focusing on Smart Cameras

The much-hyped emerging landscape of an IoT (Internet of Things) has already introduced many consumers—often of affluent and tech-savy demographics—to novel modes of interaction and smart functionality. While there are many fascinating new devices to consider, this research focuses on one: smart home security cameras. These devices exemplify a new consumer technology delicately, if not precariously, balanced along a creepy line. On one side, these devices offer security against old and new threats to the home. On the other, they introduce new vulnerabilities by subjecting the most private and intimate interior spaces to tracking and surveillance. Hanging in the balance along this secure/creepy line, smart home security cameras are striking instances of and metaphors for the contemporary growing pains, tradeoffs, and anxieties that accompany bringing smart surveillant devices into the most personal and private spaces of the home. The poetic valence is greatest with *indoor* smart security cameras, such as Amazon's Indoor Cloud Cam and Google's Indoor Nest Cam. Here, with the smart camera gaze literally pointed at the self within the home, a user may willingly subject oneself to 24-hour surveillance—and all for the ostensive purpose of increasing home security.

More Than a Camera, More than a Security Device

Reviewing the emerging landscape of smart security cameras through the concepts of digital leakage, hole-and-corner applications, and foot-in-the-door devices reveals two key trends. First, *smart security cameras are technically much more than cameras*. Today's smart security cameras automatically alert users when motion or people are detected, they allow homeowners to view live camera feeds from their phones, and some even identify individual faces. And as with many smart products, security cameras such as Nest Cam collect environmental data including device temperature and ambient light. Cloud-based subscription services such as Google's Nest Aware offer copious data storage and sophisticated data analysis. The most recent innovation is the Nest Cam's familiar face alerts, which comes with the caveat that "Depending on where you live, you may need to get consent to scan the faces of people visiting your home". Users may think they are buying a better security camera but are actually getting much more.

Second, smart security cameras offer more than security. Smart security cameras may be sold as a security camera, but marketing materials often suggest they are lifestyle or entertainment devices with analogies to social media and handheld digital cameras. For example, Nest users are invited to submit their favorite videos captured with the smart security cameras. Selected videos are posted on the Nest Videos webpage under categories that, in addition to "Security", include "Mystery Solved", "Family Moments", "Pets", "Nature", and "Timelapses." The best user submitted content is honored with "Nestie Awards" for categories such as "Best Dog in a Lead Role" and "Best Fall". Nest advertisements frequently feature pets and kids, suggesting a radically inclusive notion of "security." Users may think they are buying a camera simply for security, but ultimately it fulfills social, playful, and reflective functions.

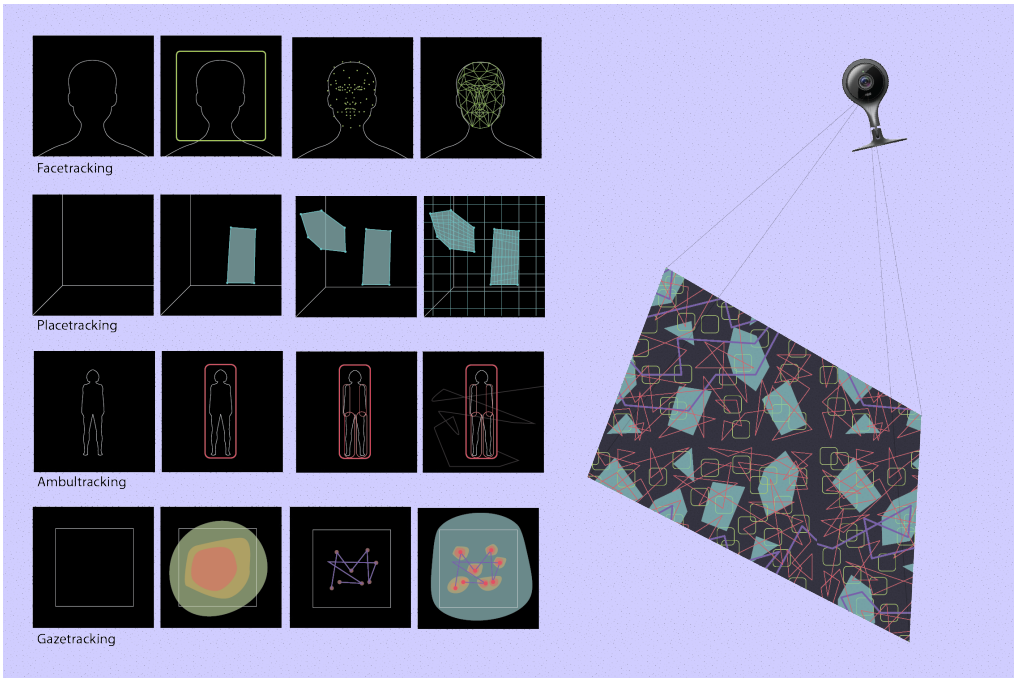


Figure 1 (left). Facetracking, Placetracking, Gazetracking, and Ambultracking [Image credit: James Pierce].A study of emerging interaction and recognition paradigms for smart cameras.
Figure 2 (right). Applications of facetracking, placetracking, gazetracking, and ambultracking.

Leaky Sensor Fields

"Information wants to be free," goes the saying famous saying often attributed to Internet pioneer Steward Brand. Years later—with the Internet thoroughly privatized and financialized—the corollary to Brand's famous claim is that digital data wants to leak. *Digital leakage* names the propensity for digital information to be shared, stolen, and misused in ways unbeknownst and possibly harmful to those to whom the data pertains, originates, or belongs. Through processes of digital leakage, seemingly private or secure digital information is surreptitiously collected, shared with additional parties, and used in unexpected and unsolicited ways. Digital leakage occurs both accidentally and intentionally, as well as both openly and secretly. Examples of leakage are diverse, and include the use of personal data for targeted third-party ads, large-scale data breaches, illegal law enforcement surveillance of smart phones, and sharing sexually explicit personal content without consent. As Shklovski et al have note, leakage is a common metaphor used in privacy and security discourses.

The design studies and explorations that follow develop the metaphor of digital leakage by focusing on specific sites and processes. This research highlights three key sites at which digital leakage occurs: *leaky sensor fields, leaky data pipelines,* and *leaky data analytics.*The following studies and explorations focus on the proliferation of leaky sensor fields created with smart home security and other smart devices.

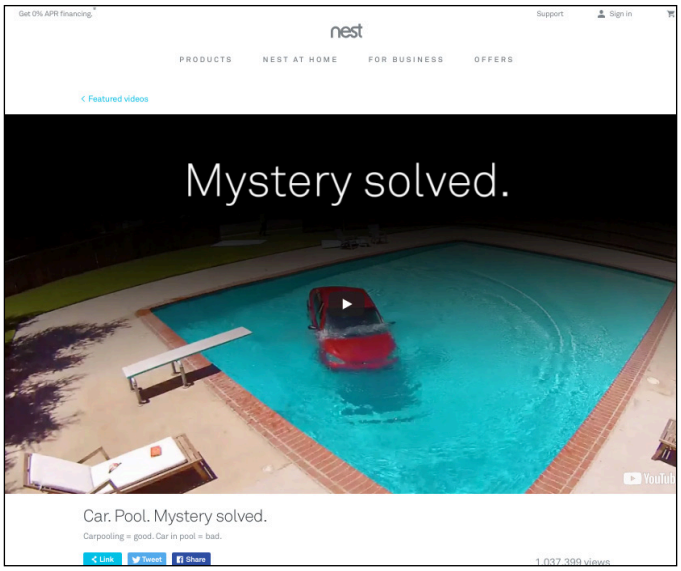


Figure 3. Nesties and #CaughtOnNest Videos The design and marketing of today's smart security cameras push the boundaries of conventional definitions of home security. An examination of marketing and advertising materials for Google's NestCam and Amazon's Cloud Cam, for example, reveals use cases that involve capturing candid and serendipitous snapshots of pets, children, and bizarre events—situations that extend well beyond the core use case scenarios of catching burglars or negligent caretakers. Google's "Best of Nest" platform nurtures these extended uses by awarding the most captivating and entertaining videos caught on Nest. The site goes so far as to suggest a new, branded subgenre of social video—the Nestie.[Image Source: Google Nest].

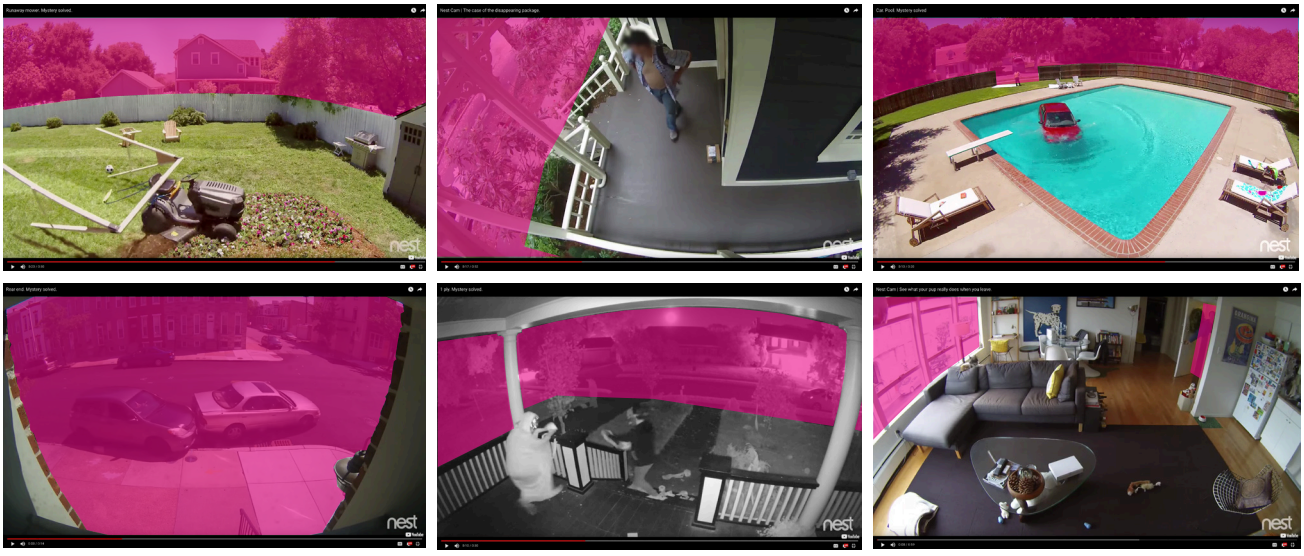


Figure 4. *Leaky #CaughtOnNest Videos* [Image credit: James Pierce]. In this design exploration user submitted videos featured on the Nest website are modified to identify camera sensor leakage spilling over fences, property lines, and window and doorway thresholds. These studies draw attention to overlooked privacy and possible legal violations lurking in the background of these wildly entertaining and awe-inspiring moments #CaughtOnNest. This analysis reveals potentials for leaky sensor fields to spread: to drip, seep, and spill over into previously unmonitored interstices and territories.

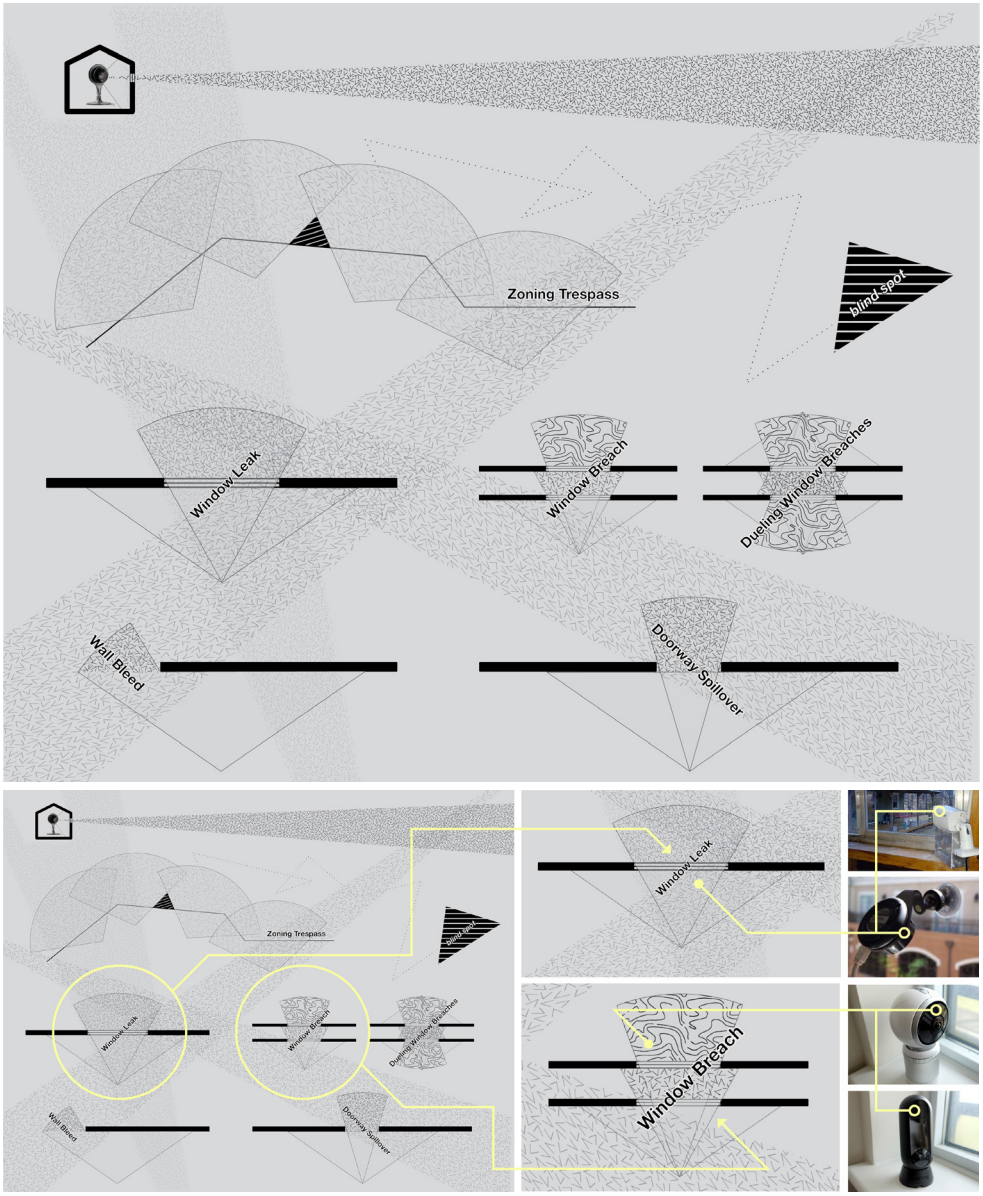


Figure 5. *Towards an Architectural Taxonomy of Leaky Sensor Fields.* [Image credit: James Pierce].

Leaky sensor fields form where the sensing capacities of smart cameras and similar devices cross socio-technical thresholds such as property lines, political boundaries, windowpanes, fences, and doorways. The inevitably pervasive leakiness occurring within neighborhoods and cities awash with smart cameras will provide ample opportunities for casual peeks into the lives of others, and for both open, feigned, and genuinely accidental surveillance of neighbors, friends, family, strangers, and ourselves. These design explorations aim to architecturally catalog and represent the emerging world of smart, leaky sensor fields. Consider, for example, the window breach where a smart camera is pointed at the window of a neighbor. The smart camera window breach does not simply allow someone to surreptitiously video record a neighbor. With a smart camera, someone can monitor the interior of a neighbors home to automatically notify them when there is activity or when it identifies a certain or unfamiliar face. In the near future, a smart camera might easily peer into a neighboring window to tell you the occupant's mood, activity levels, and whom they have been keeping company with.

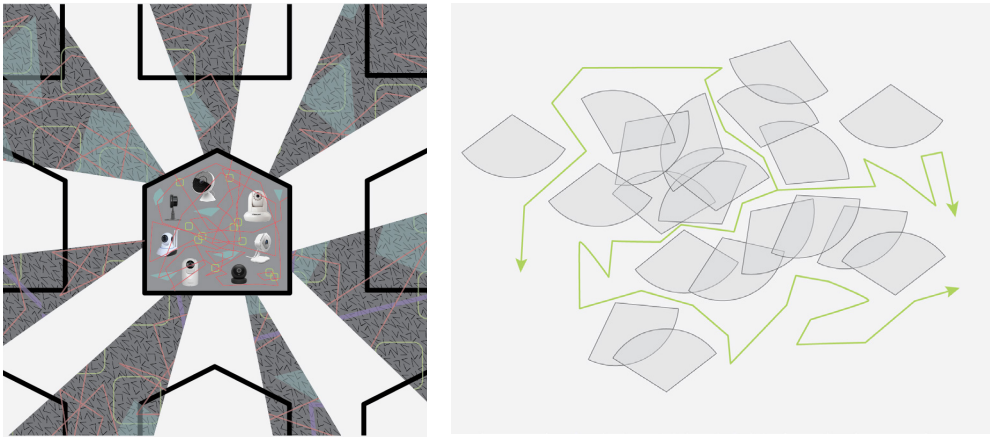


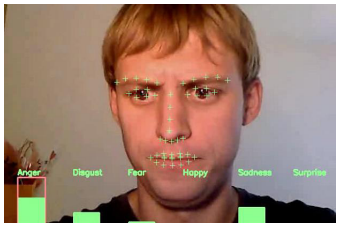
Figure 6. *Sensor Blind Spots Route Planning and Detection Devices.* [Image credit: James Pierce].

The above explorations highlight the significance of blindspots as an opportunity to combat or evade leaky sensor fields. Sensor blindspots form at the limits of a device's sensing capacities. Sensor blindspots can form at the absence of a sensing device, or can be actively produced with physical or electromagnetic interference. For example, consider the above scenarios of the window breach or window leak. In these scenarios, artistic provocations that confuse or evade facial recognition and digital camera sensors may actually soon prove practically useful in everyday contexts. For example, consider Adam Harvey's CV Dazzle digital camouflaging makeup, Neuro-Speculative Afro-Feminism's HyperFace camouflaging scarf, and Mark Shepard's camera blocking CCD-Me-Not Umbrella. *Sensor Blindspots* imagines detection and route planning tools that allow people to intricately mapped out blindspots and navigate space accordingly. Similar to how people take back streets or alleys when they want to avoid visibility, here we imagine navigation paths and points of rest influenced by sensor blindspots free from leaky sensor fields.

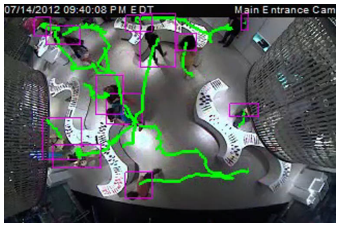
Leaky Applications. Leaky sensor fields expand the range and context of what data are collected, stored, shared, and analyzed. The following design studies consider ways that applications capitalize on digital leakage. The leakiness of digital applications if oftentimes by design. In other cases, the question of strategic intent is unclear and contentious. An illustrative example of a hole-and-corner application is when reports surfaced in 2017 that the domestic robotic vacuum cleaner Roomba was generating maps of users homes (Astor, 2017). This led to speculation that the iRoomba company might sell these maps to advertisers or other third parties. This possible scenario was reported with alarmist headlines such as "Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder" even though iRoomba assured customers it would not do so.

As a way to concretely consider emerging applications of smart leaky cameras, five controversial application areas for smart cameras are presented below: Neuromarketing, Big Data Policing, Deepfakes, Social Credit, and Quantifed Self-Surveillance. In curating these examples of actual smart camera applications, attention is given to both the visual aesthetics of tracking and surveillance and to the sensationanlism and controversy of these applications. Following Pierce and DiSalvo, this section elevates sensational, outlier examples—what they refer to as "troubling edge cases" (4-5). Pierce and DiSalvo articulate a tactic of "drawing lines between center and edge" as way of connecting the mainstream with marginal and outlier concerns.

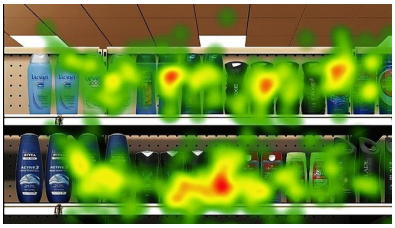
The emerging visual aesthetics of surveillance, tracking, and machine learning represented below (Figure 7) provide inspration for subsequent design proposals presented. Some proposals reference these aesthetics while others explore alternatives.



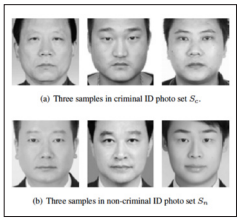
Neuromarketing: Emotion Tracking

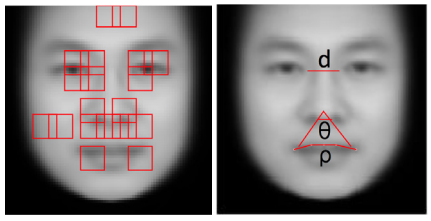


Neuromarketing: Movement Tracking

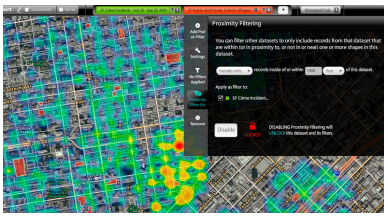


Neuromarketing: Gazetracking





Big Data Policing: Predicting Criminality from Anatomy

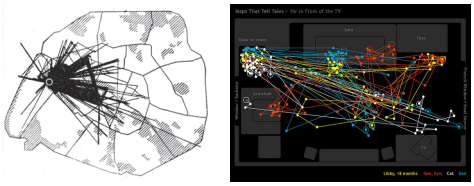


Big Data Policing: Crime Maps

Deepfakes: Fake Politician and Celebrity Videos

Social Credit: Shaming Jaywalkers and Docking Scores

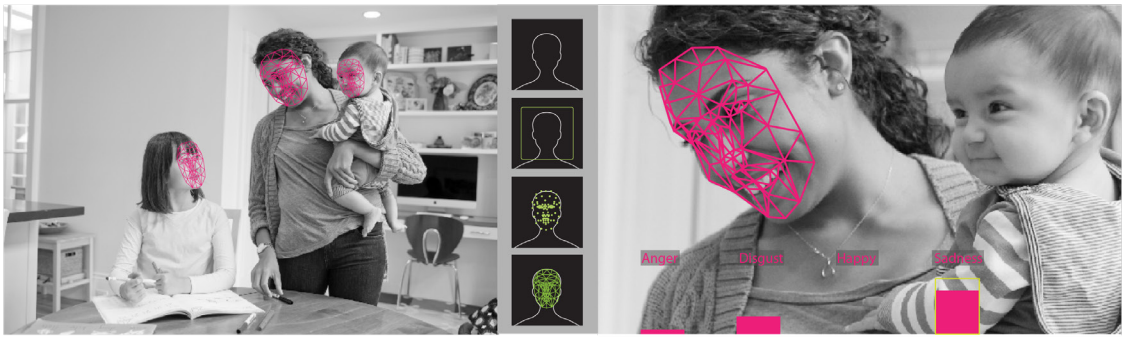
Self-Surveillance: Google Maps Histories



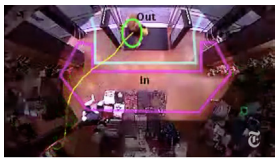
Self-Surveillance: Quantified Self Movement Mapping

Figure 7. Leaky Smart Camera Edge Case Examples. Upper left to lower right: Realeyes webcam-based emotion tracking for neuromarketing (See Clifford and Hardy, 2013); RetailNext's consumer retail tracking system (ibid); Unilever eye-tracking visualizations; Figures from Wu, Xiaolin and Zhang, Xi "Automated Inference on Criminality using Face Images." (Wu and Zhang, 2016b); PredPol® predictive policing interface; Deepfake altering the face of ex-US President Bill Clinton in actor Nicolas Cage; China docking credit scores of jaywalkers; "Google Maps Has Been Tracking Your Every Move, And There's A Website To Prove It" (Flux, 2017); French Socioligist Paul-Henry Chombart de Lauwe's (1952) study outlining the movements of a female student living in Paris during the course of a year (Pinder, 1996); Inspired by de Lauwe's map, a father manually mapped the movement of his daughter, son, and cat by carefully reviewing video footage over a period of 1 hour on Christmas 2006. See (Kelly, 2008).

Catching the nanny being sad



A domestic childcare worker is surveilled by her employer. Her behavior and emotions are monitored for erratic activity, signs of depression or anxiety, and job satisfaction. Even though she appears to be smiling, deep learning artificial intelligence closely monitors her facial expressions and determines she is actually unhappy and is likely clinically depressed. This scenario highlights a general hole-and-corner application area of emotional domestic surveillance.



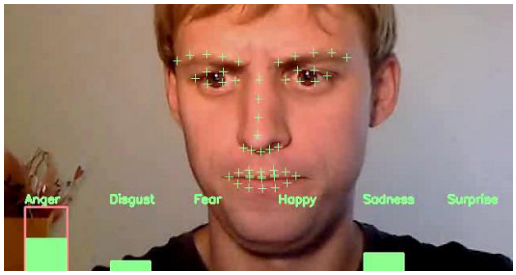


Figure 8. *Catching the Nanny Being Sad*.Example design scenario where smart home cameras are used to monitor and potentially reprimand or fire a domestic worker who is not covered by worker protection laws. [Image credit: James Pierce].

Speculative Hole-and-Corner Scenarios

How how might the troubling edge case applications areas outlined in Figure 8 play out in the future smart home? The following design explorations demonstrate a method of developing speculative scenarios by taking existing applications in areas such as Big Data Policing and Neuromarketing and applying them in domestic contexts with consumer IoT smart cameras. Figure 8 considers a scenario where a domestic worker is surveilled by her employer who uses smart cameras with machine learning to assess her mental health and well-being, her levels of fondness of the children she cares for, and her job satisfaction.

Beyond User Profiles: Interior, domestic, household, activity, and place profiles. The scenarios above further bring into focus a new development in the evolution of the user profile. User profiles are collections of data associated with a person that are used to construct models that can predict behavior. The speculative scenarios and subjects above highlight the emergence of domestic profiles, household profiles, activity profiles, and place profile. The design scenarios presented here foreground the ways in which smart home devices may work their way into the most intimate corners, hidden crevices, and darkest closets of people's lives. As one reporter writes, "the [smart home] race is not just about selling fancy appliances. It's also a fight for which company coordinates smart homes and collects data about the habits of those who live inside." (Kopytoff, 2018).

These scenarios also foreground the involvement of unwitting, uniformed, or coerced subjects. A particularly illuminating user profile to consider is a domestic worker such as nanny, caregiver, or housecleaner who, in many countries, are excluded from worker protection laws. Oftentimes it is a subject, rather than an informed, consenting, and benefiting user, who stands to lose the most or suffer the greatest harms resulting from creepy, leaky applications.

Close Interaction Studies and Speculative Roadmaps

The applications scenarios previously considerly may operate surreptitiously behind the scenes and out of the spotlight. But unwelcome or unsolicited applications and features can also emerge slowly over time. This section develops the concept of *foot-in-the-door devices*—functional offerings and affordances that lay the groundwork for the future adoption and integration of features that might have been rejected previously as unacceptable or unnecessary. An illustrative example of a foot-in-the-door device is how the smartphone created opportunities for mass-scale, and in some cases illegal, surveillance by governments and corporations. Democratic citizens and informed consumers would not voluntary carry a device in their pockets whose sole function was to track their movement and activity without offering compensation or benefits. However, the form and functions of the smartphone created foot-in-the-door potentials—or, in this case device-in-the-pocket potentials—that were later exploited and capitalized upon.

Taking "more than a camera, more than security" as a starting point, the following studies closely analyze specific features of the Indoor Nest Cam. These studies focus on physical features and affordances and how they may knowingly or unknowingly stage foot-in-the-door strategies for integrating and normalizing standalone smart cameras within the home. The selected and highly abbreviated close interaction studies that follow adapt and combine three key methodologies: design critiques [30,34,56], close readings from literary criticism [40], and mediation analysis from philosophy of technology [1,57,65,66].

At Hand- and Eye-Level | **Among Everyday Things**

Atop Books | **Recording Kids** | **Talking to Pets**

Figure 9. *Analysis of Nest Cam image staging.* Analysis excerpts showing annotated press and marketing images and video stills for the Nest Indoor Cam and Nest Cam IQ. [Image Credit: Google Nest Cam Press Images]

Tethering as Foot-in-the-Door Devices

Even though the Nest Indoor Cam is WiFi enabled, it still requires a USB cord for electrical power. Out of the box, the device comes with 9.8 foot (24.9 cm) long USB cord. In Nest support and marketing materials, this feature is advertised as benefit: "Because Nest cameras and Hello don't rely on batteries, you don't need to worry about changing them or losing your video feed if they die." But what other intentions or effects may belie this functionalist rationale for a smart "wireless" device with 10-foot power cord?

The cord subtly gives users a sense of control by allowing them to feel they securely hold control of the device—like a dog on a leash. The cord provides a simple and effective deterrent against concealment: If a hidden camera is suspected, one can easily verify the suspicion by looking for a cord attached to an outlet and then following it back to its source. Subtly, the *cord-as-leash* and *cord-as-giveaway* communicate to camera owners and subjects alike: "I am an open, honest, and safe device—totally unlike my distant cousin, the sneaky, conniving spy camera."

Face-to-Face Domestication as Foot-in-the-Door Devices

Another notable feature of the Indoor Nest Cam is its base and mounting options. The stock base can be mounted magnetically, with adhesive tape, or with screws. However, the simplest way to mount the Nest Cam is to rest it atop a flat surface and adjust to the desired angle (see Figure 9). Whereas video security cameras are typically mounted overhead on walls or ceilings, today's smart home security cameras are equipped with wide-angle lenses and pivoting bases that allow and invite them to be casually set down upon common household surfaces such as shelves, tables, countertops, desk, cubbies, and window ledges. This visible, friendly,

and human-level placements sharply contrast with the hidden spy camera or overhead security camera.

In one particularly clever and intriguing press image for the Nest IQ Cam—an upgraded model with facial recognition technology—the device is placed atop a stack of books. From bottom to top, the titles forming the stack are: The Human Figure in Motion, The Adventures of Sherlock Holmes, The Man Who Knew Too Much, and Through the Looking Glass (Figure 9). This delightful curation of titles and the ordering of the stack subtly gestures toward the security camera's own unfolding foot-in-the-door trajectory, and the anxieties and contradictions lurking beneath the camera that users must, at some level, grapple with. The Human Figure in Motion: The extraordinary abilities of cameras to see so much more about ourselves and our bodies than the naked eye alone. Sherlock Holmes: Catching criminals, solving mysteries. The Man Who Knew Too Much: When unnatural sleuthing abilities lead to the development of moral complications. Through the Looking Glass: The sequel to a classic childhood adventure that begins with a step into an alternative world and ends with the main character wondering if it was real, or if she's been living in someone else's dream.

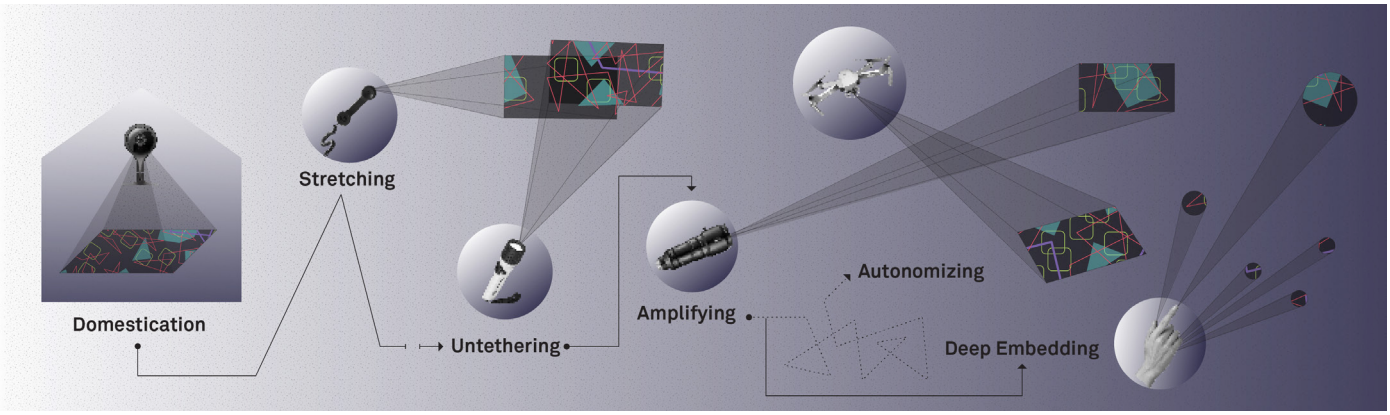


Figure 10. Speculative Foot-in-the-Door Roadmap for smart cameras beginning with the domestication of security cameras for safety and culminating in the deep embedding of cameras into pens, fingers, and cockroaches. [Image credit: James Pierce].

Speculative Foot-in-the-Door Roadmaps

Longer term, we speculate that the strategic intent of smart security cameras and other IoT is to integrate and normalize sensor devices into the most private and intimate recesses of people's lives. Security is among the most compelling reasons to invite self-surveilling device into one's home. Eventually and gradually, though, a foot-in-the-door analysis suggests that once smart home security cameras have settled in, their uses and configurations will significantly shift and expand, continuing their current foot-in-the-door plot of becoming more than cameras, and more than security devices. Given the shifts and expansions from classic security functions of catching home intruders and delinquent caregivers to capturing videos of pets and kids and living among books and furniture, the following exploration imagines a foot-in-the-door roadmap that would extend the reach and functions of smart cameras within the home.

Stretching and Untethering. The static, fixed-length power cord lengthens and eventually detaches completely. Inspired by vacuum cleaners and landline telephones—task-specific devices designed to be put away after use—we consider scenarios for smart cameras with long, retractable cords and springy, coiled cords. Designs concepts explored include mobile standalone smart camera with a snap-off magnetic power charger and handle that is designed to float around home like a remote control or a toy, or be easily carried and ready at hand like a flashlight or mobile phone.

Amplifying. Sensor amplification can develop in multiple directions: extended view angles, increased resolution, or additional sensing capabilities such as lidar or GPS. Concepts explored include a smart security camera retrofitted with a telescopic lens and directional microphone—possibly for a neighborly law enforcement surveillance scenario outlined previously.

Autonomizing. Once untethered, smart cameras may begin to robotically pivot, swivel, and rove. Autonomous movement further amplifies sensing capacities. Concepts explored include a Roomba-inspired roving camera and swarms of camera pocket drones.

Deep embedding. When miniaturization and wireless power are combined with untethering and amplifying, smart camera become deeply embedded into surfaces and objects. This embedding creates unprecedented opportunities for concealment, mobility, and extended reach. Concepts explored include smart camera em-

Figure 11. Clips. [Image Credit: Google Press images]

Since this project began in early 2017, Google Clips—a miniature clip-on camera—was released for sale in 2018. Clips represents a clear first step along the above roadmap that begins with stretching and untethering.

Smart Home Redirects

In this section I illustrate the three redirective design tactics devised and applied within the research through design process. These tactics are redirective in the sense of moving beyond near-term incremental improvements that align with status quo or dominant design trajectories. These tactics direct design imagination along three vectors: *divergently* into the absurd and exaggerated, *accelerating* past plausible or expected near-term projections, and productively *restraining* and reversing the ratcheting up effects of technological advancement. This method is generally useful for considering how smart devices, homes, and environments might unfold. This method has proved particularly useful for considering future design possibilities that lie between the outlandish, the alarming, and the resolving. This approach can be helpful in avoidin the extremes of unwavering criticality and unreflective solutionism.

Smart Home Deviations

What if we extrapolate a foot-in-the-door roadmap to absurd endpoints? Showcasing a redirective tactic of playful smart home divergence, this work deliberately dwells upon bizarre and exaggerated scenarios tinged with absurdity and humor. Social media, domestic appliances, and home décor serve as inspirational design metaphors and analogous experiences. A snapshot of divergent scenarios presented below imagine smart camera use cases expanding beyond home security to fulfill playful, social, reflective, and decorative functions—operating as much more than either a camera or a security device.

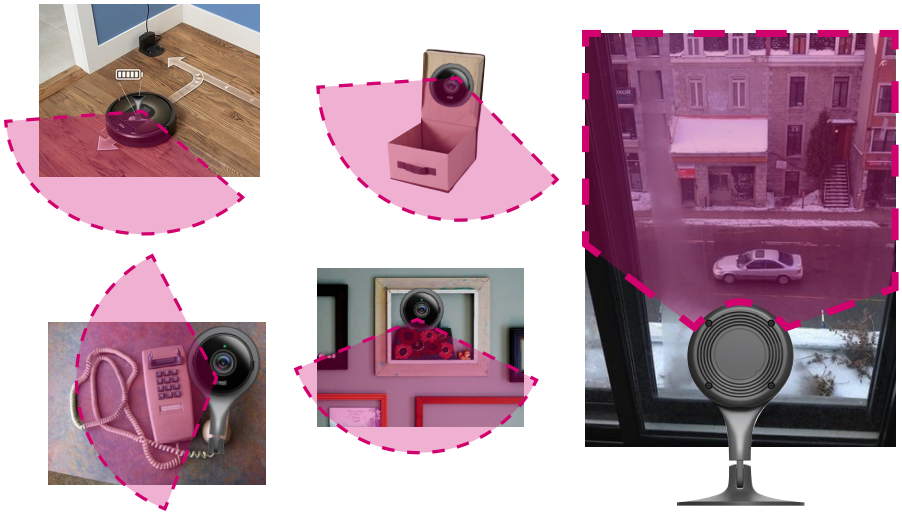


Figure 12. *Nest Cam+ Deviations.* Roving Coverage: Cam + Roomba Robotic Vacuum. Honeypot Trap: Cam + Box. Extendable Eye: Cam + Landline Telephone. Decorative Surveillance: Nest + Decorative Cam. Front Window: Cam + Window Sill. [Image credit: James Pierce]

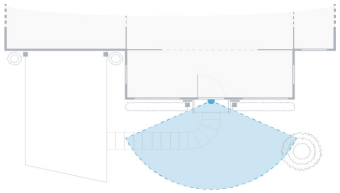


Figure 13. Nest Cam instructional material.[Image Credit: Nest Press Image]

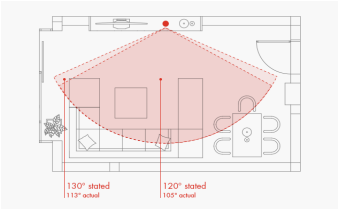


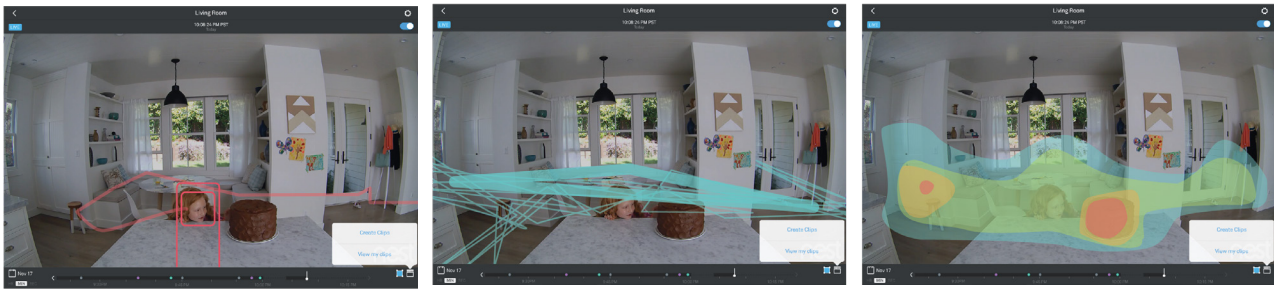
Figure 14. Analysis of advertised versus actual Nest Cam view angle. [Image Credit: Pet Gear Lab]

Smart Home Acceleration

What if today's speculative hole-and-corner applications and foot-in-the-door trajectories continue to rapidly develop and soon emerge as normal, accepted, even indispensible aspects of life? Here we consider scenarios where smart cameras and their leaky, surveillant gazes become as normal and pervasive as electric lighting. When electricity was first introduced into homes over 100 years ago, some were fearful that it would leak out and cause physical harm. Nowadays, electric lighting is an accepted and necessary feature of modern life. Lamps and lighting function as an intriguing metaphor for imagining a future awash in utterly normal and mundane smart camera coverage. Employing a redirective tactic of smart home acceleration, these design explorations push the boundaries of what is today considered acceptable, useful, and desirable.

Smart Home Restrainment

What if severe public backlash amid a succession of hole-and-corner and foot-in-the-door scandals leads to substantial curtailment, regulation, and increased user control options of smart technologies? These explorations consider increased controls and protections from ubiquitous smart cameras and other leaky technologies. These interventions range in scale from device features to legislation. The redirective design tactic of smart home restrainment is used to generate counterbalancing forces capable of combating rampant digital leakage pervading things, bodies, homes, and environments. The design metaphors of curtains and shutoffs figure prominently.



Activity Tracks (2)
Bedroom
11:02 - 1:39 AM

Activity Deleted
Bedroom
11:02 - 1:39 AM

Family Activity
Kitchen
2018

Mom's Activity
Entire House
5/15/2019 1:20-2:00

Cat's Activity
All Cameras
Yesterday

Figure 14. *Quantified Self Decor: Data-Selfies and Auto-Selfies.* **These** speculative scenarios explore a world in which personal and household data from facetracking, gazetracking, placetracking, and ambultacking creates interesting, evocative, and aesthetic patterns of data which may or may not have clear pragmatic uses. This explorations specifically explores concepts for Data-Selfies and Auto-Selfies. These scenarios imagine Quantified Self gone "mainstream" and "social" at once. [Image credit: James Pierce.]

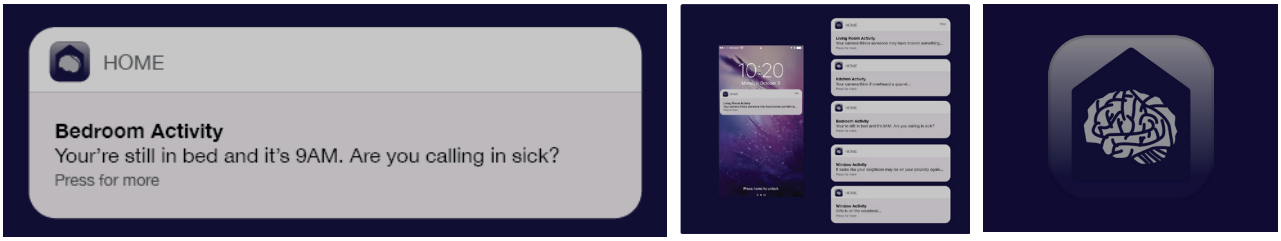


Figure 15. *Very Personal Alerts, Intimate Cam Analysis, and Smart Home Chatter.* As intelligent camera gets smarter, they will be able to increasingly infer intimate personal details. In a Wired review article of the Nest camera, the author speculates on the future of smart homes cameras: "In the future, Nest says the [face recognation] Cam IQ will offer integration with both Google Home and Amazon Alexa, creating a network of devices that constantly watch and listen and oversee our lives at home. The possibilities there are still to be determined, but it seems likely that in the near future, we'll be able to say, 'OK Google, what's mom cooking for dinner?' and our machines will know the answer" (Pardes, 2017). We might also be able to ask it "How is mom feeling?", "What did my partner do yesterday", and "Am I depressed?" and receive accurate, detailed, and sometimes shocking answers. [Image credit: James Pierce.]

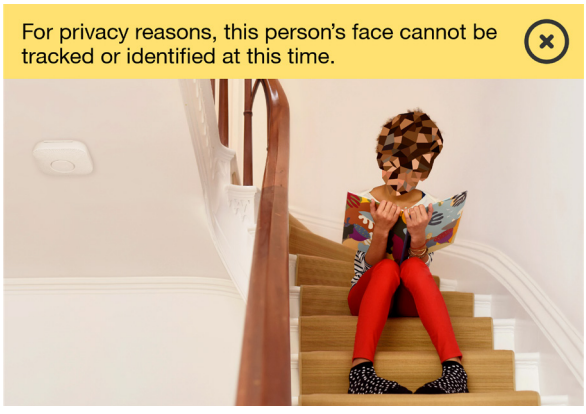


Figure 16. **D***o No Facetrack Registries.* National "Do Not Call" databases and similar programs that allow people to opt out of unscolicited telemarketing calls emerged in response to early 2000s legislation in Canada, the UK, the US, and other countries. As more everyday technologies employ faceprinting and tracking, concerns may lead to analogous legislation allowing people to limit the extent to which they can be identified, tracked, and surviellied by smart cameras. [Image credit: James Pierce.]

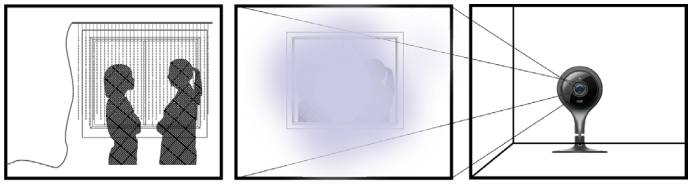


Figure 17. *CCD-Me-Not Curtains.* [Image credit: James Pierce]. Inspired by Mark Shepard's camera-blocking CCD-Me-Not Umbrella (Sheperd, 2008), we find a domestic application for infrared LED light interference techniques to disrupt the peering smart camera of neighbors or passersby.

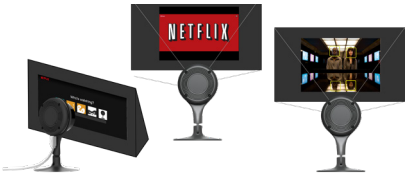


Figure 18. *Mistraining Sessions.* Research has shown smart camera cyberattacks could reveal when the camera detects motion, indicating someone may be home, even when the traffic is encrypted (Apthorpe, 2016). Reports that iRobot might share maps of customers' homes gleaned from data collected by the Roomba robotic vacuum spurred discussions about what information could be revealed through smart home devices (Astor, 2017). As a data obfuscating practice (Brunton, 2015), smart camera mistraining sessions might help to foil attackers by corrupting leaky data. [Image credit: James Pierce].

Lamps and Lighting as Design Metaphors for Smart Home Accelerationism

The scenarios of aesthetic, playful, and social self-surveillance presented previously would require more ubiquitous domestic self-surveillance infrastracture. Here we explore some possible configurations of an expanded domestic camera and sensor infrastructure that would allow smart home camera coverage to spread into the most intimate and private of spaces, such as bedrooms, bathrooms, desktops, and closets.

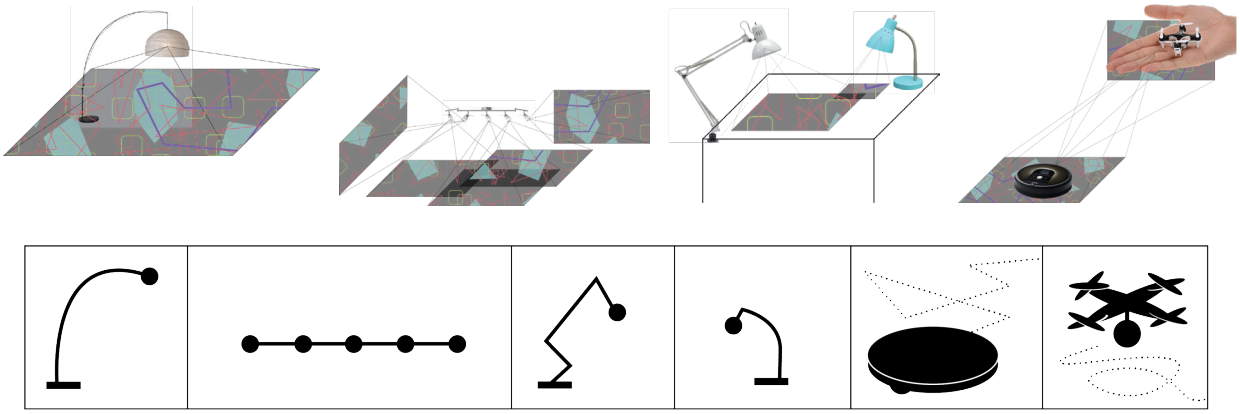


Figure 19. *What if Future Smart Cameras are as Normal, Ubiquitous, and Useful as Electric Lighting?* These proposals explore smart cam configurations based on ambient, accent, and task lighting, along with new modes of roving and autonomous IoT.[Image Credit: James Pierce.]

The design explorations below explore lamps and lighting as design metaphors for imagining how smart cameras might practically integrate and socially normalize within daily life. Lamps and lighting offer powerful interactive and architectural metaphor for envisioning a future of domestic surveillance designed to shine onto the most private recesses of our lives and illuminate our most intimate behaviors, thoughts, and desires. Future smart home cameras may operate with similarities to household lamps both in form and function. The diversity of common house lamp forms—from overhead track lighting to arced floor lamps to focused desk lamps—offer ready-made base configurations for smart home cameras.

Future smart home cameras may operate with similarities to household lamps both in form and function. The diversity of common house lamp forms—from overhead track lighting to arced floor lamps to focused desk lamps—offer ready-made base configurations for smart home cameras that support wall-to-wall and precision camera coverage. Lighting analogies help us think through the ways that self-surveillance of the future may serve illuminating, decorative, and mood-setting functions that demand ubiquitous coverage along with precision placement and directional control.

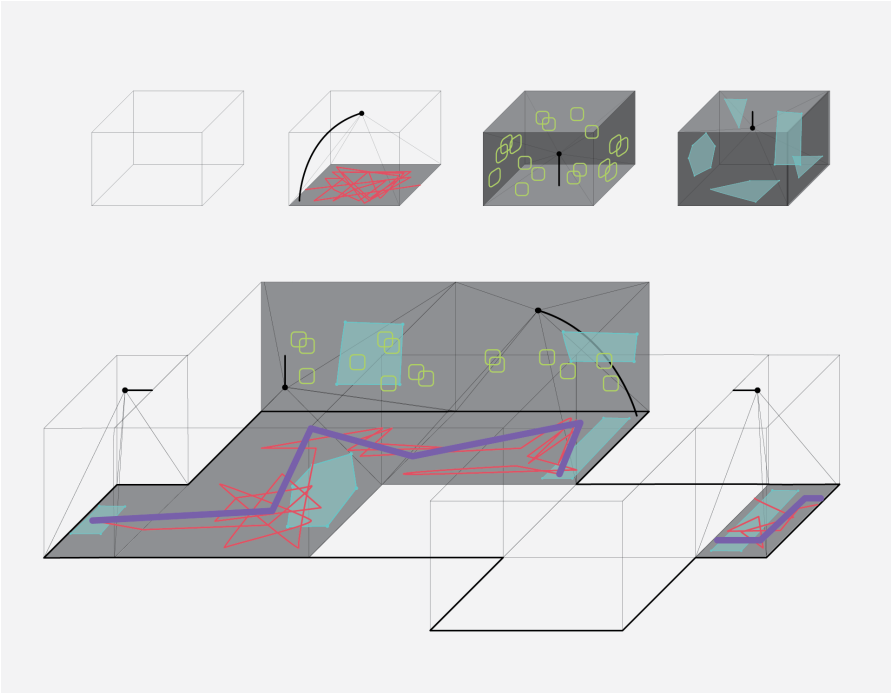


Figure 20. *Wall-to-Wall and Precision Coverage.* If smart home camera surveillance spreads into the most intimate and private spaces such bedrooms, tabletops, and closets, the physical infrastructure that enables this will likely involve two major categories of lighting-inspired supports. *Wall-to-wall* coverage provides uniform coverage for entire spaces, similar to ambient light provided by overhead and floor lamps. *Precision coverage* pinpoints specific areas, activities, and timeframes. It operates like task and accent lighting provided by desklamps, headlamps, and more novel and sophisticated automated and autonomous lighting devices.[Image Credit:James Pierce.[

Curtains and Shutoffs

As potential antitode to the proliferation of leaky sensor fields as normal and ubiquitous as electric lighting, *curtains* and *shuttoffs* serves as potent metaphors for designing blindspots, obfuscations, and user controls.

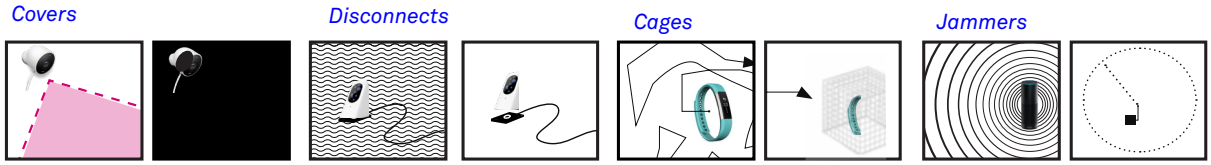


Figure 21. *Active, Passive, and Deactive Smart Device Restraints.* [Image Credit: James Pierce.]

Smart Product Collage Kits

The prior explorations led to the development of smart product collage kits:physical, operational compositions that combined two or more existing off-the-shelf consumer products or other discernible cultural or technological forms.

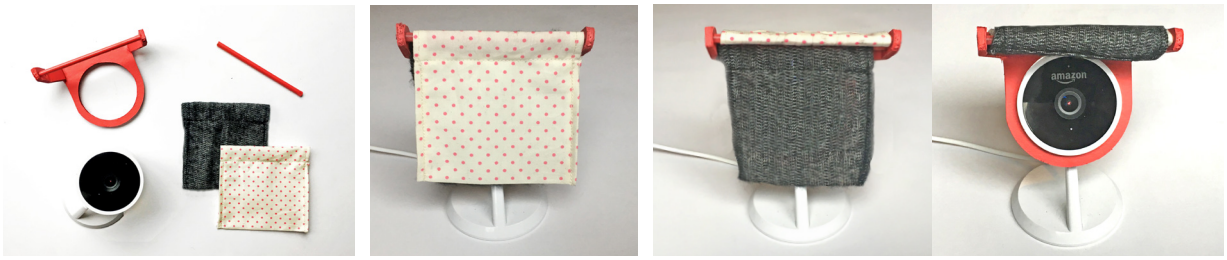


Figure 22. *Amazon Cloud Cam Curtains Kit.* [Image Credit: James Pierce.]

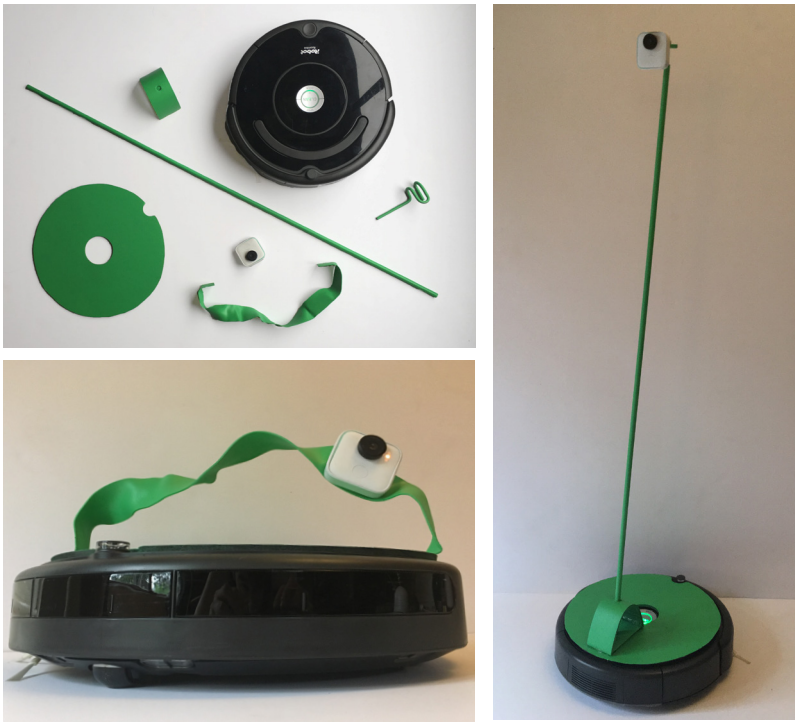


Figure 23. *Roomba Clips Cam Kit*
[Image Cedit: James Pierce.]

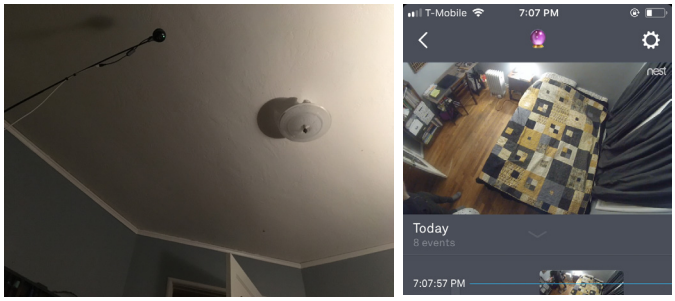
Figure 24. *IKEA Arc Lamp Nest Cam Kit.* [Image Credit: James Pierce.]

Within these product collages, two design principles are at work : **(1) Conceptual redirection:** Construct product collages that push existing products along alternative developmental trajectories. Accelerate, amplify, restrain, exaggerate, deviate, etc. **(2) Anchored speculation.** Construct product collages that clarify and expose, rather than obscure, the products (i.e., compositional elements) that are being conceptually redirected. This anchors speculation to salient reference points, and draws implicit lines between imagined futures and present actualities.

Ongoing Field Studies

These prototypes are currently being deployed with participants and used by the designers. Below is a sample of anectodotes that highlight emergent concerns, habits, etiquette, pleasures, obsessions, and other activites. By designing to both accelerate and restrain, we prompt people to examine and explore the positives, negatives, and manifold ambiguities of smart cams.

I put it in my bedroom.
It immediately, instinctually shamed me into making my bed.

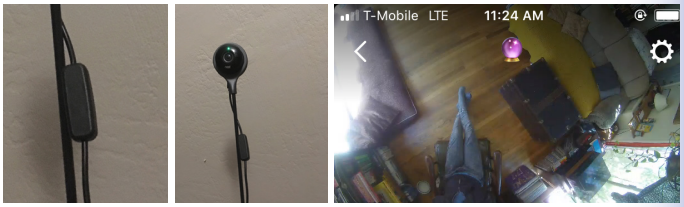


I put them where my cat naps.
I check on her incessantly.

What if it watches me eat breakfast?

Figure 24. *Ikea Arc Lamp Nest Cam.*[Image Credit: James Pierce.]

The third-party USB power switch means I know for sure it's OFF.



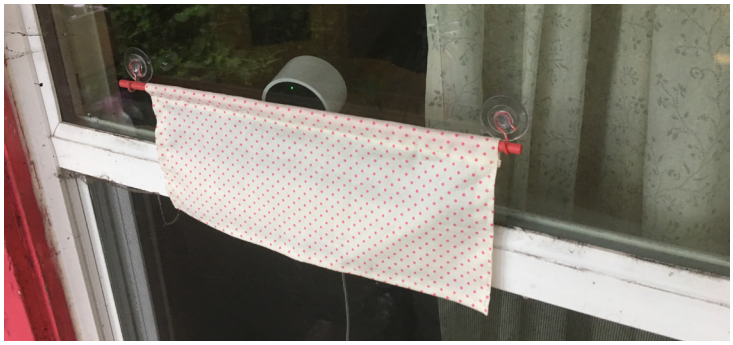


Figure 24. *Amazon Cloud Cam Curtains.*[Image Credit: James Pierce.]

References

Astor, M. (2017) "Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared." The New York Times.

Cole, R. Google Eric Schmidt - The Creepy Line (Edited). Accessed September 17, 2018. https://www.youtube.com/watch?v=mp-mOL-MT5lQ.

Davoli, L., Wiltse, H., and Redström, J. (2015) Trojans & Drones: Materializing possibilities for transforming industrial infrastructures. Proceedings of RtD '15.

Giaccardi, E., Speed, C., Cila, N., & Caldwell, M. (2016) Things as co-ethnographers: Implications of a thing perspective for design and anthropology. Design Anthropological Futures, 235.

Jenkins, T. (2018) "Cohousing IoT: Design Prototyping for Community Life." Proceedings of TEI '18. ACM.

Kopytoff, V. (2014) "The Real Reason Google Paid $3.2 Billion For Nest." Time.

Pierce, J. (2019) "Smart Home Security Cameras and Shifting Lines of Creepiness: A Design-Led Inquiry." Proceedings ofCHI '19. ACM.

Pierce, J., and DiSalvo, C. (2018) "Addressing Network Anxieties with Alternative Design Metaphors." Proceedings of CHI '18. ACM.

Shklovski, I., Mainwaring, S., Skúladóttir, H., and Borgthorsson, H. (2014) "Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use." Proceedings of CHI '14. ACM.

Wakkary, R., Oogjes, D., Lin, H,, and Hauser, S. (2018) "Philosophers Living with the Tilting Bowl." Proceedings of CHI '18. ACM.